MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Guía para #StopRansomware

Publicado: mayo de 2023

Historial de modificaciones

Versión	Fecha	Revisión/Descripción de la modificación	Sección/Página afectada
1.0	Septiembre de 2020	Primera versión	
2.0	Mayo de 2023	Véase "Novedades" en la pág. 3	Actualizaciones

INTRODUCCIÓN

El ransomware es una forma de malware diseñado para cifrar archivos en un dispositivo, inutilizándolos a ellos y a los sistemas que dependen de ellos. Los delincuentes exigen un rescate a cambio del descifrado. Con el tiempo, los delincuentes han adaptado sus tácticas para que el ransomware sea más destructivo y con mayor impacto, también han exfiltrado datos de las víctimas y las han presionado para que paguen amenazándolas con hacer públicos los datos robados. La aplicación de ambas tácticas se conoce como "doble extorsión". En algunos casos, los delincuentes pueden exfiltrar datos y amenazar con liberarlos como su única forma de extorsión sin emplear ransomware.

Estos incidentes de ransomware y violación de datos asociados pueden afectar gravemente a los procesos empresariales al dejar a las organizaciones incapaces de acceder a los datos necesarios para operar y prestar servicios cruciales de misión. El impacto económico y reputacional del ransomware y la extorsión de datos ha demostrado ser un reto costoso para las organizaciones de todos los tamaños a lo largo de la interrupción inicial y, a veces, la recuperación extendida.

Esta guía es una actualización de la Guía sobre ransomware de la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) y el Centro Interestatal de Análisis e Intercambio de Información (MS-ISAC) publicada en septiembre de 2020 (véase Novedades) y fue desarrollada a través del JRTF. Esta guía incluye dos recursos principales:

Esta guía ha sido elaborada por el Grupo de trabajo conjunto contra el ransomware de los Estados Unidos (JRTF).

El JRTF, copresidida por la CISA y el FBI, es un esfuerzo de colaboración entre agencias para combatir la creciente amenaza de los ataques de ransomware. El JRTF se puso en marcha en respuesta a una serie de ataques de ransomware de alto perfil contra infraestructuras cruciales y agencias gubernamentales estadounidenses. El JRTF:

- Coordina y agiliza la respuesta del gobierno de los EE. UU. a los ataques de ransomware y facilita el intercambio de información y la colaboración entre las agencias gubernamentales y los socios del sector privado.
- Garantiza la coordinación operativa de actividades como el desarrollo y el intercambio de mejores prácticas para prevenir y responder a los ataques de ransomware, las investigaciones y operaciones conjuntas contra los autores de amenazas de ransomware, y la orientación y provisión de recursos a las organizaciones que han sido víctimas de ransomware.
- Representa un avance importante para permitir la unidad de esfuerzos en todas las iniciativas del gobierno de los EE. UU. para hacer frente a la creciente amenaza de los ataques de ransomware.

Para más información sobre el JRTF, consulte cisa.gov/joint-ransomware-task-force.

- Parte 1: Prácticas recomendadas para la prevención del ransomware y la extorsión de datos
- Parte 2: Lista de comprobación de la respuesta al ransomware y la extorsión de datos

La Parte 1 proporciona orientación a todas las organizaciones para reducir el impacto y la probabilidad de incidentes de ransomware y extorsión de datos, incluyendo las mejores prácticas para prepararse, prevenir y mitigar estos incidentes. Las mejores prácticas de prevención se agrupan por vectores

comunes de acceso inicial. La Parte 2 incluye una lista de comprobación de las mejores prácticas para responder a estos incidentes.

Estas mejores prácticas y recomendaciones de prevención y respuesta ante el ransomware y la extorsión de datos se basan en los conocimientos operativos de la CISA, el MS-ISAC, la Agencia de Seguridad Nacional (NSA) y la Oficina Federal de Investigación (FBI), en lo sucesivo denominadas organizaciones autoras. El público de esta guía incluye profesionales de tecnología de la información (TI), así como otras personas dentro de una organización involucradas en el desarrollo de políticas y procedimientos de respuesta a incidentes cibernéticos o en la coordinación de respuesta a incidentes cibernéticos.

Las organizaciones autoras recomiendan que las organizaciones tomen las siguientes medidas iniciales para preparar y proteger sus instalaciones, personal y clientes de las amenazas a la seguridad cibernética y física y otros peligros:

- Unirse a un centro sectorial de intercambio y análisis de información (ISAC), cuando sea elegible, como:
    - MS-ISAC para entidades gubernamentales estatales, locales, tribales y territoriales (SLTT) de EE. UU. - learn.cisecurity.org/ms-isac-registration. La afiliación al MS-ISAC está abierta a representantes de los 50 estados, el Distrito de Columbia, los territorios de EE. UU., los gobiernos locales y tribales, las entidades públicas de educación K-12, las instituciones públicas de educación superior, las autoridades y cualquier otra entidad pública no federal de los Estados Unidos.
    - Centro de Análisis e Intercambio de Información sobre Infraestructuras Electorales (EI-ISAC) para organizaciones electorales de EE. UU. - learn.cisecurity.org/ei-isac-registration.

      Para más información, consulte el Consejo Nacional de ISAC.
- Póngase en contacto con la CISA en CISA.JCDC@cisa.dhs.gov para colaborar en el intercambio de información, mejores prácticas, evaluaciones, ejercicios y mucho más.
- Póngase en contacto con su oficina local del FBI para obtener una lista de puntos de contacto (POC) en caso de incidente cibernético.

Colaborar con organizaciones homólogas y con la CISA permite a su organización recibir información crucial y oportuna, así como acceder a servicios para controlar el ransomware y otras ciberamenazas.

Novedades

Desde la publicación inicial de la Guía de ransomware en septiembre de 2020, los creadores de ransomware han acelerado sus tácticas y técnicas.

Para mantener la relevancia, añadir perspectiva y maximizar la eficacia de esta guía, se han hecho las siguientes modificaciones:

- Se han añadido el FBI y la NSA como coautores por sus contribuciones y visión operativa.
- Se incorporó la campaña #StopRansomware en el título.
- Se han añadido recomendaciones para prevenir los vectores de infección iniciales más comunes, incluidas las credenciales comprometidas y las formas avanzadas de ingeniería social.
- Se actualizaron las recomendaciones para tratar las copias de seguridad en la nube y la arquitectura de confianza cero (ZTA).
- Se amplió la lista de comprobación de respuesta al ransomware con consejos de caza de amenazas para su detección y análisis.
- Se ajustaron las recomendaciones a los objetivos intersectoriales en materia de ciberseguridad (CPG) de la CISA.

> #StopRansomware es el esfuerzo de la CISA y el FBI para publicar avisos para los defensores de la red que detallan información sobre defensa de la red relacionada con diversas variantes de ransomware y creadores de amenazas. Visite stopransomware.gov para obtener más información y leer los avisos conjuntos.

Parte 1: Prácticas recomendadas para la preparación, prevención y mitigación del ransomware y la extorsión de datos

Estas mejores prácticas recomendadas se alinean con los CPG desarrollados por la CISA y el Instituto Nacional de Normas y Tecnología (NIST). Los CPG proporcionan un conjunto mínimo de prácticas y protecciones que la CISA y el NIST recomiendan que todas las organizaciones implementen. La CISA y el NIST basaron los CPG en marcos y guías de ciberseguridad existentes para proteger contra las amenazas, tácticas, técnicas y procedimientos más comunes y con mayor impacto. Para más información sobre los CPG y las protecciones básicas recomendadas, visite los objetivos intersectoriales en materia de ciberseguridad de la CISA.

Preparación ante incidentes de ransomware y extorsión de datos

Consulte las mejores prácticas y referencias mencionadas en esta sección para ayudar a controlar los riesgos que plantea el ransomware e impulsar una respuesta coordinada y eficiente para su organización en caso de incidente. Aplique estas prácticas en la mayor medida posible en función de la disponibilidad de recursos de la organización.

- **Mantenga copias de seguridad cifradas, sin conexión, de los datos cruciales**, y compruebe regularmente la disponibilidad e integridad de las copias de seguridad en un escenario de recuperación de desastres [CPG 2.R]. Compruebe los procedimientos de copia de seguridad de forma regular. Es importante que las copias de seguridad sean sin conexión, ya que muchas variantes de ransomware intentan encontrar y posteriormente borrar o cifrar las copias de seguridad accesibles para hacer imposible su restauración a menos que se pague el rescate.

  Las copias de seguridad automatizadas en la nube pueden no ser suficientes, ya que si un atacante cifra los archivos locales, estos archivos se sincronizarán con la nube y posiblemente sobrescribirán los datos no afectados.

  - Mantenga y actualice regularmente "imágenes doradas" de sistemas cruciales. Esto incluye mantener "plantillas" de imágenes que tengan un sistema operativo (OS) preconfigurado y aplicaciones de software asociadas que puedan desplegarse rápidamente para reconstruir un sistema, como una máquina virtual o un servidor [CPG 2.O].
    - Utilice la infraestructura como código (IaC) para desplegar y actualizar los recursos de la nube y mantenga copias de seguridad de los archivos de plantillas sin conexión para volver a desplegar rápidamente los recursos. El código IaC debe estar controlado por versiones y los cambios en las plantillas deben auditarse.
    - Almacene el código fuente o los ejecutables aplicables con copias de seguridad sin conexión (así como los contratos de custodia y licencia). Reconstruir a partir de imágenes del sistema es más eficiente, pero algunas imágenes no se instalarán correctamente en hardware o plataformas diferentes; tener acceso independiente al software ayuda en estos casos.
  - Conserve el hardware de reserva para reconstruir los sistemas si no se prefiere reconstruir el sistema primario.
    - Considere la posibilidad de sustituir el hardware obsoleto que impide la restauración por hardware actualizado, ya que el hardware anterior puede presentar obstáculos de instalación o compatibilidad al reconstruir a partir de imágenes.
  - Considere la posibilidad de utilizar una solución multi-nube para evitar depender de un proveedor en las copias de seguridad de nube a nube en caso de que todas las cuentas del mismo proveedor se vean afectadas.
    - Algunos proveedores de servicios en la nube ofrecen soluciones de almacenamiento inmutable que pueden proteger los datos almacenados sin necesidad de un entorno independiente. Utilice el almacenamiento inmutable con precaución, ya que no cumple los criterios de conformidad de determinadas normativas y una mala configuración puede suponer un costo significativo.

- **Cree, mantenga y ejercite regularmente un plan básico de respuesta a incidentes cibernéticos (IRP) y un plan de comunicaciones asociado que incluya procedimientos de respuesta y notificación** para incidentes de ransomware y extorsión/violación de datos [CPG 2.S]. Garantice la disponibilidad de una copia impresa del plan y una versión sin conexión.
    - Asegúrese de que los procedimientos de notificación de violación de datos cumplan la legislación estatal aplicable. Consulte la Conferencia Nacional de Legislaturas Estatales: Leyes de Notificación de Violación de la Seguridad para obtener información sobre las leyes de notificación de las violaciones de datos de cada estado y consulte a un asesor jurídico cuando sea necesario.
    - En el caso de filtraciones que afecten a información sanitaria electrónica, es posible que tenga que notificarlo a la Comisión Federal de Comercio (FTC) o al Departamento de Salud y Servicios Humanos (HHS) de EE. UU. y, en algunos casos, a los medios de comunicación. Para más información, consulte la Regla de Notificación de Infracciones Sanitarias de la FTC y la Regla de Notificación de Infracciones del HHS.
    - En el caso de filtraciones que afecten a información personal identificable (PII), notifíquelo a las personas afectadas para que puedan tomar medidas que reduzcan la posibilidad de que su información sea utilizada indebidamente. Indique el tipo de información expuesta, recomiende medidas correctivas y facilite la información de contacto pertinente.
    - Notifique a las empresas de una infracción si se roba PII almacenada en nombre de otras empresas.
    - Garantice que el IRP y el plan de comunicación sean revisados y aprobados por escrito por el CEO, o equivalente, y que ambos sean revisados y comprendidos por toda la cadena de mando.
    - Revise la guía de respuesta a incidentes disponible, como la Lista de comprobación de respuesta al ransomware de esta guía y el Manual de respuesta a incidentes cibernéticos del sector público para:
        - Ayudar a su organización a organizarse mejor en torno a la respuesta a incidentes cibernéticos.
        - Crear un borrador de las declaraciones de retención de incidentes cibernéticos.
        - Desarrollar un IRP cibernético.
    - Incluya en el plan de comunicación los procedimientos de comunicación de la organización, así como plantillas para las declaraciones de retención de incidentes cibernéticos. Llegue a un consenso sobre qué nivel de detalle es apropiado compartir dentro de la organización y con el público y cómo fluirá la información.
- **Implemente una arquitectura de confianza cero** para impedir el acceso no autorizado a datos y servicios. Haga que la aplicación del control de acceso sea lo más detallada posible. La ZTA asume que una red está comprometida y proporciona una colección de conceptos e ideas diseñados para minimizar la incertidumbre a la hora de aplicar decisiones de acceso precisas y con los mínimos privilegios por solicitud en los sistemas y servicios de información.

Prevención y mitigación de incidentes de ransomware y extorsión de datos

Consulte las mejores prácticas y referencias mencionadas en esta sección para ayudar a prevenir y mitigar los incidentes de ransomware y extorsión de datos. Las mejores prácticas de prevención se agrupan por vectores comunes de acceso inicial de los creadores del ransomware y la extorsión de datos.

Vector de acceso inicial: vulnerabilidades y errores de configuración en Internet

- **Lleve a cabo una exploración regular de vulnerabilidades para identificar y tratar las vulnerabilidades**, especialmente las de los dispositivos orientados a Internet, para limitar la superficie de ataque [CPG 1.E].
    - La CISA ofrece un servicio gratuito de exploración de vulnerabilidades y otras evaluaciones gratuitas: cisa.gov/cyber-resource-hub [CPG 1.F].
- **Aplique parches y actualice periódicamente el software y los sistemas operativos a las últimas versiones disponibles**.
    - Dé prioridad a la aplicación oportuna de parches en los servidores orientados a Internet (que utilizan software para procesar datos de Internet, como navegadores web, complementos de navegadores y lectores de documentos), especialmente para detectar vulnerabilidades conocidas.
    - Las organizaciones autoras, conscientes de las dificultades que tienen las pequeñas y medianas empresas para mantener actualizados los servidores orientados a Internet, instan a migrar los sistemas a proveedores de nube "gestionados" de confianza para reducir, no eliminar, las funciones de mantenimiento de los sistemas de identidad y correo electrónico. Para más información, visite la página de información sobre ciberseguridad de la NSA, Mitigar las vulnerabilidades de la nube.
- **Asegúrese de que todos los dispositivos locales, de servicios en la nube, móviles y personales (es decir, BYOD) estén configurados correctamente y que las funciones de seguridad estén activadas**. Por ejemplo, desactive los puertos y protocolos que no se utilicen con fines empresariales (por ejemplo, el protocolo de escritorio remoto [RDP] - el protocolo de control de transmisión [TCP], Puerto `3389`) [CPG 2.X].
    - Reduzca o elimine los despliegues manuales y codifique la configuración de los recursos en la nube mediante IaC. Compruebe las plantillas de IaC antes del despliegue con herramientas de análisis de seguridad estática para identificar errores de configuración y brechas de seguridad.
    - Compruebe de forma rutinaria si hay cambios en la configuración para identificar los recursos que se modificaron o introdujeron fuera de la implantación de plantillas, reduciendo así la probabilidad de que se introduzcan nuevas brechas de seguridad y configuraciones erróneas. Aproveche los servicios de los proveedores de la nube para automatizar o facilitar la auditoría de los recursos con el fin de garantizar una línea de base coherente.

- **Limite el uso del RDP y otros servicios de escritorio remoto**. Si el RDP es necesario, aplique las mejores prácticas. Los creadores de amenazas a menudo obtienen acceso inicial a una red a través de servicios remotos expuestos y mal protegidos, y más tarde atraviesan la red utilizando el cliente nativo RDP de Windows. Los creadores de amenazas también suelen obtener acceso explotando redes privadas virtuales (VPN) o utilizando credenciales comprometidas. Infórmese en la Consultoría de la CISA: Seguridad en una VPN empresarial.
    - Audite la red en busca de sistemas que utilicen un RDP, cierre los puertos RDP no utilizados, aplique bloqueos de cuentas tras un número determinado de intentos, aplique una autenticación multifactor (MFA) y registre los intentos de inicio de sesión con el RDP.
    - Actualice las VPN, los dispositivos de infraestructura de red y los dispositivos utilizados para acceder remotamente a los entornos de trabajo con los últimos parches de software y configuraciones de seguridad. Implemente la MFA en todas las conexiones VPN para aumentar la seguridad. Si no se implementa la MFA, exija a los trabajadores remotos que utilicen contraseñas de 15 caracteres o más.
- **Deshabilite las versiones 1 y 2 del protocolo de bloque de mensajes del servidor (SMB)** y actualice a la versión 3 (SMBv3) después de mitigar las dependencias existentes (por parte de los sistemas o aplicaciones existentes) que puedan romperse al deshabilitarlo. Los delincuentes utilizan el SMB para propagar malware a través de las organizaciones, por lo que se debe endurecer el SMBv3:
    - Bloquee o limite el tráfico del SMB interno a los sistemas que requieren acceso. Esto debería limitar las intrusiones que se mueven lateralmente a través de su red.
    - Implemente la firma del SMB. Esto debería evitar ciertos ataques de tipo adversary-in-the-middle y pass-the-hash. Para obtener más información, consulte Mitigating New Technology Local Area Network (LAN) Manager (NTLM) Relay Attacks on Active Directory Certificate Services (AD CS) y Overview of Server Message Block Signing en Microsoft.
    - Bloquee el acceso externo del SMB a su red bloqueando el puerto TCP `445` con los protocolos relacionados en los puertos `137`–`138` del protocolo de datagramas de usuario (UDP) y el puerto TCP `139`.
    - Implemente el cifrado del SMB con la Convención de Nomenclatura Universal (UNC) para los sistemas que admiten esta función. Esto debería limitar la posibilidad de ataques de escucha e interceptación.
    - Registre y supervise el tráfico del SMB para ayudar a detectar comportamientos potencialmente anómalos.

Vector de acceso inicial: credenciales comprometidas

- **Implementar una MFA resistente al phishing en todos los servicios**, en particular para el correo electrónico, las VPN y las cuentas que acceden a sistemas cruciales [CPG 2.H]. Informar a la alta dirección cuando se descubran sistemas que no permitan la MFA, sistemas que no apliquen la MFA y usuarios que no estén registrados con la MFA.

    - **Considere la posibilidad de emplear una MFA sin contraseña** que sustituya las contraseñas por dos o más factores de verificación (por ejemplo: una huella dactilar, el reconocimiento facial, el pin del dispositivo o una clave criptográfica).

- **Considere la posibilidad de suscribirse a servicios de supervisión de credenciales** que vigilan la red oscura en busca de credenciales comprometidas.
- **Implemente sistemas de gestión de identidades y accesos (IAM)** para proporcionar a los administradores las herramientas y tecnologías necesarias para supervisar y gestionar las funciones y los privilegios de acceso de entidades de red individuales para aplicaciones locales y en la nube.
- **Implemente un control de acceso de confianza cero** creando políticas de acceso sólidas para restringir el acceso de usuario a recurso y de recurso a recurso. Esto es importante para los recursos de gestión de claves en la nube.
- **Cambiar los nombres de usuario y contraseñas de administrador por defecto** [CPG 2.A].
- **No utilice cuentas de acceso root para las operaciones cotidianas**. Cree usuarios, grupos y funciones para llevar a cabo tareas.
- **Implemente políticas de contraseñas que requieran contraseñas únicas de al menos 15 caracteres**. [CPG 2.B] [CPG 2.C].

    - Los gestores de contraseñas pueden ayudarlo a desarrollar y gestionar contraseñas seguras. Asegure y limite el acceso a cualquier gestor de contraseñas en uso y active todas las funciones de seguridad disponibles en el producto en uso, como la MFA.

- **Aplique políticas de bloqueo de cuentas después de un cierto número de intentos fallidos de inicio de sesión**. Registre y supervise los intentos de inicio de sesión para el descifrado de contraseñas por fuerza bruta y la pulverización de contraseñas [CPG 2.G].
- **Almacene las contraseñas en una base de datos segura y utilice algoritmos hash sólidos**.
- **Desactive el almacenamiento de contraseñas en el navegador en la consola de administración de políticas de grupo**.
- **Implemente la solución de contraseña del administrador local (LAPS)** siempre que sea posible si su sistema operativo es anterior a Windows Server 2019 y Windows 10, ya que estas versiones no tienen LAPS integrado. **Nota:** Las organizaciones autoras recomiendan que las organizaciones actualicen a Windows Server 2019 y Windows 10 o superior.
- Proteja contra el dumping del servicio de subsistema de autoridad de seguridad local (LSASS):

    - **Implemente la regla de reducción de superficie de ataque (ASR) para el LSASS.**
    - **Implemente Credential Guard para Windows 10 y Server 2016**. Consulte Microsoft Manage Windows Defender Credential Guard para más información. Para Windows Server 2012R2, habilite la verificación ligera de proceso protegido (PPL) para la autoridad de seguridad local (LSA).

- **Eduque a todos los empleados sobre la seguridad adecuada de las contraseñas en su capacitación anual sobre seguridad**, haciendo hincapié en no reutilizar las contraseñas y no guardarlas en archivos locales.

- **Utilice Windows PowerShell Remoting, Remote Credential Guard o RDP** con modo de administración restringido cuando establezca una conexión remota para evitar la exposición directa de las credenciales.
- **Separe las cuentas de administrador de las cuentas de usuario** [CPG 2.E]. Sólo permita que las cuentas de administrador designadas sean usadas para propósitos administrativos. Si un usuario individual necesita derechos administrativos sobre su estación de trabajo, utilice una cuenta separada que no tenga acceso administrativo a otros hosts, como servidores. Para algunos entornos de nube, separe las funciones cuando la cuenta utilizada para aprovisionar/gestionar claves no tenga permiso para utilizar las claves y viceversa. Como esta estrategia introduce una sobrecarga de gestión adicional, no es apropiada en todos los entornos.

Vector de acceso inicial: phishing

- **Implemente un programa de concienciación y capacitación sobre ciberseguridad para los usuarios** que incluya orientación sobre cómo identificar y reportar actividades sospechosas (por ejemplo, phishing) o incidentes [CPG 2.I].
- **Marque los correos electrónicos externos en los clientes de correo electrónico**.
- **Implemente filtros en la puerta de enlace del correo electrónico para filtrar correos electrónicos** con indicadores maliciosos conocidos, como líneas de asunto maliciosas conocidas, y bloquear direcciones de protocolo de Internet (IP) sospechosas en el cortafuegos [CPG 2.M].
- **Active los filtros de archivos adjuntos comunes para restringir los tipos de archivos que suelen contener malware** y que no deben enviarse por correo electrónico. Para más información, consulte la publicación de Microsoft Anti-malware protection in EOP.
    - Revise los tipos de archivos de su lista de filtros al menos cada semestre y añada otros tipos de archivos que se hayan convertido en vectores de ataque. Por ejemplo, los archivos adjuntos de OneNote con malware incrustado se han utilizado recientemente en campañas de phishing.
    - Los malware suelen comprimirse en archivos protegidos por contraseña que eluden los escáneres antivirus y los filtros de correo electrónico.

> La CISA ofrece una evaluación gratuita de campañas de phishing y otras evaluaciones gratuitas. Visite cisa.gov/cyber-resource-hub.

- **Implemente la política y verificación por autenticación basada en dominios para mensajes, informes y conformidad (DMARC)** para reducir la posibilidad de que se suplanten o modifiquen correos electrónicos de dominios válidos. La DMARC protege su dominio de la suplantación de identidad, pero no protege de los correos electrónicos entrantes que han sido suplantados, a menos que el dominio remitente también implemente una DMARC. La DMARC se basa en los protocolos ampliamente implantados de convenio de remitentes (SPF) y de correo identificado con claves de dominio (DKIM), añadiendo una función de reporte que permite a remitentes y receptores mejorar y supervisar la protección del dominio frente al correo electrónico fraudulento. Para más información sobre la DMARC, consulte CISA Insights Enhance Email & Web Security y el blog del Center for Internet Security How DMARC Advances Email Security.

  Malicious Domain Blocking and Reporting (MDBR) es un servicio gratuito para organizaciones SLTT financiado por CISA, MS-ISAC y EI-ISAC. Este servicio de seguridad totalmente gestionado impide que los sistemas informáticos se conecten a dominios web dañinos y protege contra las ciberamenazas, entre las que se incluyen:

  - Malware,
  - Ransomware y
  - Phishing.

  Para inscribirse en MDBR, visite cisecurity.org/ms-isac/services/mdbr/.

- **Asegúrese de que las secuencias de comandos de macros están desactivadas para los archivos de Microsoft Office transmitidos por correo electrónico**. Estas macros pueden utilizarse para enviar ransomware [CPG 2.N]. **Nota:** Las versiones recientes de Office están configuradas por defecto para bloquear los archivos que contengan macros de Visual Basic para aplicaciones (VBA) y mostrar una barra de confianza con una advertencia de que las macros están presentes y se han desactivado. Para más información, consulte Macros from the internet will be blocked by default in Office en Microsoft. Consulte Block macros from running in Office files from the Internet en Microsoft para obtener instrucciones de configuración para desactivar las macros en archivos externos para versiones anteriores de Office.
- **Desactive el alojamiento de scripts de Windows (WSH)**. El alojamiento de scripts de Windows proporciona un entorno en el que los usuarios pueden ejecutar scripts o realizar tareas.

Vector de acceso inicial: infección de malware precursor

- **Utilice actualizaciones automáticas para su software antivirus y antimalware y sus firmas**. Asegúrese de que las herramientas estén correctamente configuradas para escalar las advertencias y los indicadores a fin de notificar al personal de seguridad. Las organizaciones autoras recomiendan utilizar una solución antivirus de gestión centralizada. Esto permite detectar tanto el malware "precursor" como el ransomware.
    - Una infección de ransomware puede ser la prueba de un compromiso previo de la red no resuelto. Por ejemplo, muchas infecciones de ransomware son el resultado de infecciones de malware ya existentes, como QakBot, Bumblebee y Emotet.
    - En algunos casos, el despliegue del ransomware es el último paso para comprometer una red y se deja caer para ocultar actividades previas posteriores al compromiso, como comprometer el correo electrónico empresarial (BEC).

> La CISA y el MS-ISAC animan a las organizaciones SLTT a utilizar Albert IDS para mejorar una estrategia de defensa a profundidad. Albert sirve como una capacidad de alerta temprana para los gobiernos SLTT de EE. UU. y apoya la conciencia situacional y la defensa de la ciberseguridad a nivel nacional. Para más información sobre Albert, visite cisecurity.org/services/albert-network-monitoring/.

- **Utilice listas de aplicaciones permitidas o soluciones de detección y respuesta de puntos finales (EDR)** en todos los activos para garantizar que sólo se puede ejecutar el software autorizado y que se bloquee todo el software no autorizado.
    - En Windows, active Windows Defender Application Control (WDAC), AppLocker o ambos en todos los sistemas que admitan estas funciones.
        - WDAC está en continuo desarrollo, mientras que AppLocker sólo recibirá correcciones de seguridad. AppLocker se puede utilizar como complemento de WDAC, cuando WDAC se establece en el nivel más restrictivo posible, y AppLocker se utiliza para ajustar las restricciones para su organización.
    - Utilice listas de permisos en lugar de intentar enumerar y denegar todas las posibles permutaciones de aplicaciones en un entorno de red.
    - Considere la posibilidad de implementar una EDR para los recursos en la nube.
- **Considere la posibilidad de implementar un sistema de detección de intrusiones (IDS)** para detectar la actividad de mando y control y otras actividades de red potencialmente maliciosas que se producen antes de la implantación del ransomware.
    - Asegurarse de que el IDS se supervise y gestione de forma centralizada. Configure correctamente las herramientas y dirija las advertencias y los indicadores al personal adecuado para que tome las medidas oportunas.
- **Supervise los indicadores de actividad y bloquee la creación de archivos maliciosos con la utilidad Sysmon de Windows**. A partir de Sysmon 14, la opción `FileBlockExecutable` puede utilizarse para bloquear la creación de ejecutables maliciosos, archivos de biblioteca de vínculos dinámicos (DLL) y archivos de sistema que coincidan con valores hash específicos.

Vector de acceso inicial: Formas avanzadas de ingeniería social

- **Cree políticas que incluyan capacitación de concienciación en ciberseguridad** sobre formas avanzadas de ingeniería social para el personal que tenga acceso a su red. La capacitación debe incluir consejos sobre cómo reconocer sitios web y resultados de búsqueda ilegítimos. También es importante repetir periódicamente la capacitación de concienciación sobre seguridad para mantener al personal informado y alerta.
- **Implemente un sistema de nombres de dominio (DNS) de protección.** Al bloquear la actividad maliciosa de Internet en su origen, los servicios de DNS de protección pueden proporcionar una alta seguridad de red a los trabajadores remotos. Estos servicios de seguridad analizan las consultas DNS y toman medidas para mitigar amenazas (como malware, ransomware, ataques de phishing, virus, sitios maliciosos y spyware) aprovechando el protocolo y la arquitectura DNS existentes. Los SLTT pueden implementar el servicio MDBR sin costo alguno. Consulte el documento Selecting a Protective DNS Service. **de la NSA y la CISA.**
- **Considere la posibilidad de implantar navegadores aislados** para proteger los sistemas de programas maliciosos procedentes de la navegación web. Los navegadores aislados aíslan la máquina del código malicioso.

Entre las formas avanzadas de ingeniería social se incluyen:

- Envenenamiento de optimización de motores de búsqueda (SEO), también conocido como envenenamiento de búsqueda: cuando los delincuentes crean sitios web maliciosos y utilizan tácticas de SEO para que aparezcan de forma destacada en los resultados de búsqueda. El envenenamiento de SEO secuestra los resultados de los motores de búsqueda de sitios web populares e inyecta enlaces maliciosos para impulsar su posicionamiento en los resultados de búsqueda. Estos enlaces conducen a los usuarios desprevenidos a sitios de phishing, descargas de malware y otras ciberamenazas.
- Descargas no autorizadas (sitios web impostores): cuando un usuario descarga involuntariamente código malicioso al visitar un sitio web aparentemente legítimo que es malicioso. Los delincuentes utilizan las descargas no autorizadas para robar y recopilar información personal, inyectar troyanos o introducir kits de exploits u otros programas maliciosos en los puntos finales. Los usuarios pueden visitar estos sitios respondiendo a un correo electrónico de phishing o haciendo clic en una ventana emergente engañosa.
- "Malvertising": publicidad maliciosa que los ciberdelincuentes utilizan para inyectar malware en los ordenadores de los usuarios cuando éstos visitan sitios web maliciosos o hacen clic en un anuncio en línea. La publicidad maliciosa también puede dirigir a los usuarios a un sitio web dañado en el que se pueden robar sus datos o descargar programas maliciosos en su ordenador. La publicidad maliciosa puede aparecer en cualquier parte, incluso en sitios que usted visita como parte de su navegación web cotidiana.

Vector de acceso inicial: Terceros y Proveedores de servicios gestionados

- **Considere las prácticas de manejo de riesgos e higiene cibernética de terceros o proveedores de servicios gestionados (MSP)** en los que confía su organización para cumplir su misión. Los MSP han sido un vector de infección de ransomware que ha afectado a numerosas organizaciones clientes [CPG 1.I].
    - Si un tercero o MSP es responsable de mantener y proteger las copias de seguridad de su organización, asegúrese de que siguen las mejores prácticas aplicables descritas anteriormente. Utilice el lenguaje contractual para formalizar sus requisitos de seguridad como práctica recomendada.

> Los delincuentes pueden aprovecharse de las relaciones de confianza que su organización mantiene con terceros y MSP.
>
> - Los delincuentes pueden atacar a los MSP con el objetivo de poner en riesgo a las organizaciones clientes de los MSP; pueden utilizar las conexiones de red de los MSP y el acceso a las organizaciones clientes como vector clave para propagar malware y ransomware.
> - Los delincuentes pueden suplantar la identidad o utilizar cuentas de correo electrónico en riesgo asociadas con entidades con las que su organización tiene una relación de confianza para realizar phishing a sus usuarios, lo que permite atacar la red y revelar información.

- **Garantice el uso del mínimo privilegio y la separación de funciones a la hora de configurar el acceso de terceros**. Los terceros y los MSP solo deben tener acceso a los dispositivos y servidores que estén dentro de su función o responsabilidades.
- **Considere la posibilidad de crear políticas de control de servicios (SCP) para los recursos basados en la nube con el fin de impedir que los usuarios o funciones, en toda la organización, puedan acceder a servicios específicos o realizar acciones específicas dentro de los servicios.** Por ejemplo, la SCP puede utilizarse para restringir a los usuarios la posibilidad de eliminar registros, actualizar configuraciones de nube privada virtual (VPC) y cambiar configuraciones de registro.

Buenas prácticas generales y Guía para el fortalecimiento de la seguridad

- **Asegúrese de que su organización cuenta con un enfoque integral de** gestión de activos [CPG 1.A].
    - Comprenda y realice un inventario de los activos informáticos de su organización, lógicos (por ejemplo, datos, software) y físicos (por ejemplo, hardware).
    - Conozca qué datos o sistemas son más críticos para la salud y la seguridad, la generación de ingresos u otros servicios críticos, y comprenda cualquier interdependencia asociada (por ejemplo, "la lista de sistemas "A" utilizada

> **Consejo:** A fin de facilitar el rastreo de activos, utilice la Hardware and Software Asset Tracking Spreadsheet de MS-ISAC.

para realizar "X" se almacena en el activo crítico "B"""). Esto ayudará a su organización a determinar las prioridades de restauración en caso de que se produzca un incidente. Aplique controles o salvaguardias de seguridad más exhaustivos a los activos críticos. Esto requiere la coordinación de toda la organización.
    - Asegúrese de que almacena la documentación de sus activos informáticos de forma segura y conserve copias de seguridad sin conexión y físicas in situ.

- **Aplique el principio de mínimo privilegio a todos los sistemas y servicios** a fin de que los usuarios sólo tengan el acceso que necesitan para realizar su trabajo [CPG 2.E]. Los delincuentes a menudo aprovechan las cuentas privilegiadas para ataques de ransomware en toda la red.
    - Restrinja los permisos de los usuarios para instalar y ejecutar aplicaciones de software.
    - Restrinja los permisos de usuario/función para acceder o modificar los recursos basados en la nube.
    - Limite las acciones que pueden realizar determinados usuarios/funciones en las claves gestionadas por los clientes.
    - Bloquee el acceso remoto a las cuentas locales mediante el uso de la política de grupo para restringir el inicio de sesión en la red por parte de las cuentas locales. Para obtener orientación, consulte Blocking Remote Use of Local Accounts y Security identifiers de Microsoft.
    - Utilice Windows Defender Remote Credential Guard y el modo de administración restringida para las sesiones RDP.
    - Elimine las cuentas y grupos innecesarios y restrinja el acceso root.
    - Controle y limite la administración local.
    - Audite Active Directory (AD) en busca de privilegios excesivos en cuentas y afiliación a grupos.
    - Utilice el grupo de usuarios protegidos de AD en los dominios de Windows a fin de proteger aún más las cuentas de usuarios con privilegios frente a los ataques pass-the-hash.
    - Audite trimestralmente las cuentas de usuario y de administrador en busca de cuentas inactivas o no autorizadas. Dé prioridad a la revisión de las cuentas de supervisión y gestión remotas de acceso público, incluidas las auditorías de los accesos de terceros concedidos a los MSP.

- **Asegúrese de que todos los hipervisores y la infraestructura informática asociada, incluidos los componentes de red y almacenamiento, estén actualizados** y reforzados. Las nuevas estrategias de ransomware han empezado a dirigirse a los servidores VMware ESXi, los hipervisores y otras herramientas y sistemas centralizados, lo que permite el cifrado rápido de la infraestructura a escala. Para obtener más información sobre la resistencia al ransomware y el fortalecimiento de VMware y otras infraestructuras de virtualización, consulte:
    - Publicación especial del NIST (SP 800-125A Rev.1): Security Recommendations for Server-based Hypervisor Platforms
    - VMware: Cloud Infrastructure Security Configuration & Hardening)

- **Aproveche las mejores prácticas y active la configuración de seguridad en asociación con entornos en la nube**, como Microsoft Office 365.
    - Revise el modelo de responsabilidad compartida para la nube y asegúrese de comprender en qué consiste la responsabilidad del cliente cuando se trata de la protección de activos.
    - Realice copias de seguridad de los datos con frecuencia; sin conexión o aproveche las copias de seguridad de nube a nube.
    - Habilite el registro de todos los recursos y establezca alertas para usos anormales.
    - Active la protección contra borrado o el bloqueo de objetos en los recursos de almacenamiento que suelen ser objetivo de ataques de ransomware (por ejemplo, almacenamiento de objetos, almacenamiento de bases de datos, almacenamiento de archivos y almacenamiento de bloques) a fin de evitar que los datos se borren o sobrescriban, respectivamente.
    - Considere la posibilidad de activar el control de versiones para mantener almacenadas múltiples variantes de los objetos. Esto permitirá una recuperación más sencilla de acciones no intencionadas o malintencionadas.
    - Cuando se admita, al utilizar el acceso programático personalizado a la nube, utilice solicitudes de interfaz de programación de aplicaciones (API) firmadas para verificar la identidad del solicitante, proteger los datos en tránsito y protegerse contra otros ataques, como los ataques de repetición.
    - Para obtener más información, consulte Consultoría de Ciberseguridad de CISA Microsoft Office 365 Security Recommendations .
- **Mitigue el uso malintencionado del** software de acceso remoto y de supervisión y gestión remotas (RMM)
    - Audite las herramientas de acceso remoto de su red para identificar el software de RMM actual o autorizado.
    - Revise los registros de ejecución del software de RMM para detectar usos anormales, o software de RMM ejecutándose como un ejecutable portátil.
    - Utilice software de seguridad para detectar casos en los que el software de RMM sólo se carga en la memoria.
    - Exija que las soluciones de RMM autorizadas sólo se utilicen desde dentro de su red a través de soluciones de acceso remoto aprobadas, como VPN o interfaces de escritorio virtual (VDI).
    - Bloquee las conexiones entrantes y salientes en los puertos y protocolos comunes de RMM en el perímetro de la red.
- **Emplee medios lógicos o físicos de segmentación de red mediante la implementación** de la ZTA y la separación de varias unidades de negocio o recursos departamentales de TI dentro de su organización y mantenga la separación entre TI y tecnología operativa [CPG 2.F]. La segmentación de la red puede ayudar a contener el impacto de cualquier intrusión que afecte a su organización y a prevenir o limitar el movimiento lateral por parte de delincuentes. La segmentación de la red puede volverse ineficaz si se viola por error del usuario o por no apegarse a las políticas de la organización (por ejemplo, conectar medios de almacenamiento extraíbles u otros dispositivos a múltiples segmentos).

- **Elabore y actualice periódicamente el(los) diagrama(s)s de red exhaustivo(s) que describa(n) los sistemas y flujos de datos dentro de la red o redes de** su organización (véase Figura 1) [CPG 2.P]. Esto es útil en estado estacionario y puede ayudar al personal de respuesta a incidentes a entender dónde centrar sus esfuerzos. Véase Figura 2 y Figura 3 para las representaciones de una red plana (no segmentada) y de una red segmentada con las mejores prácticas.
    - El diagrama debe incluir representaciones de las principales redes, cualquier esquema específico de direccionamiento IP y la topología general de la red, incluidas las conexiones de red, las interdependencias y el acceso concedido a terceros, MSP y conexiones de nube desde puntos finales externos e internos.
    - Asegúrese de almacenar de forma segura la documentación de la red y conserve copias de seguridad sin conexión e impresas in situ.

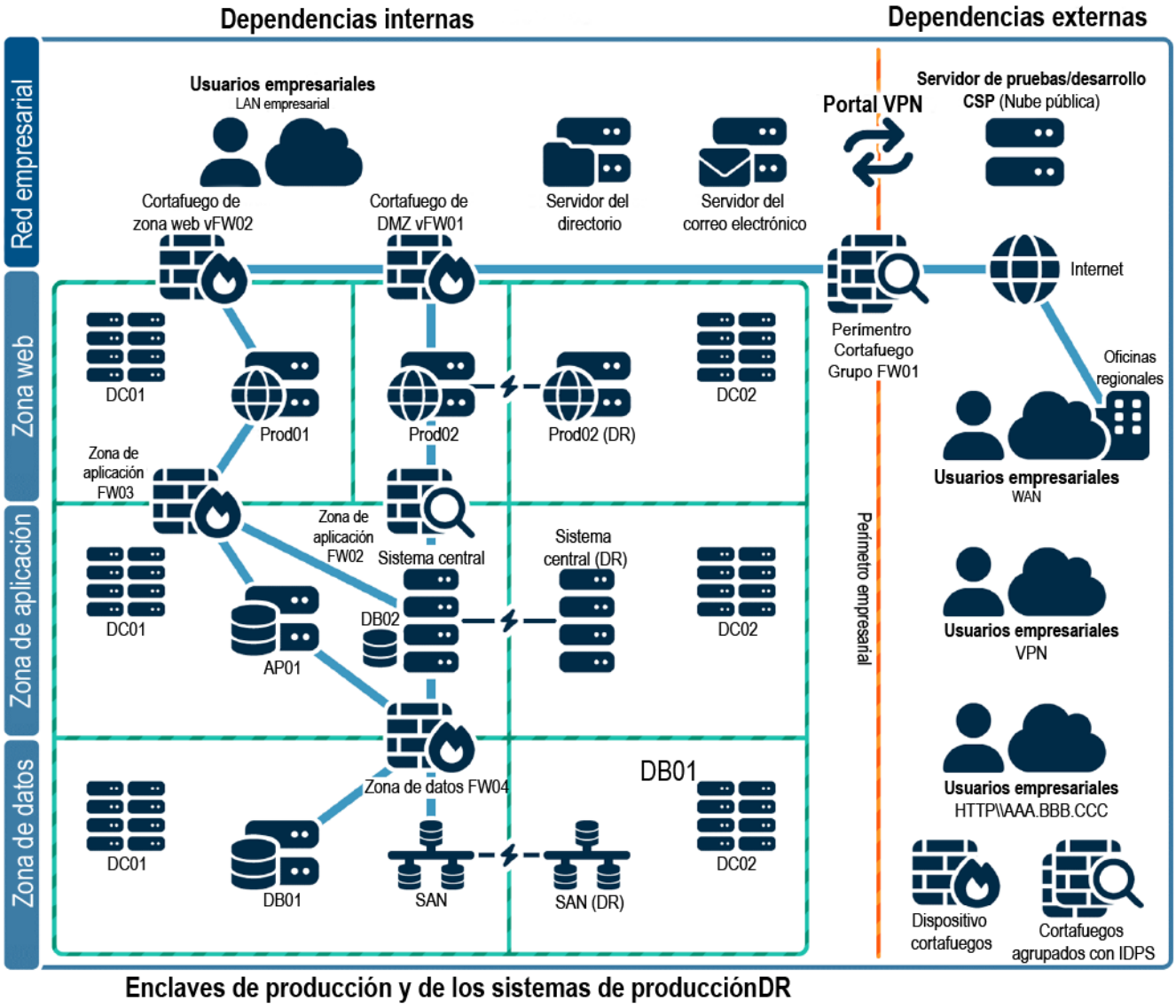

Figura 1: Ejemplo de diagrama de red

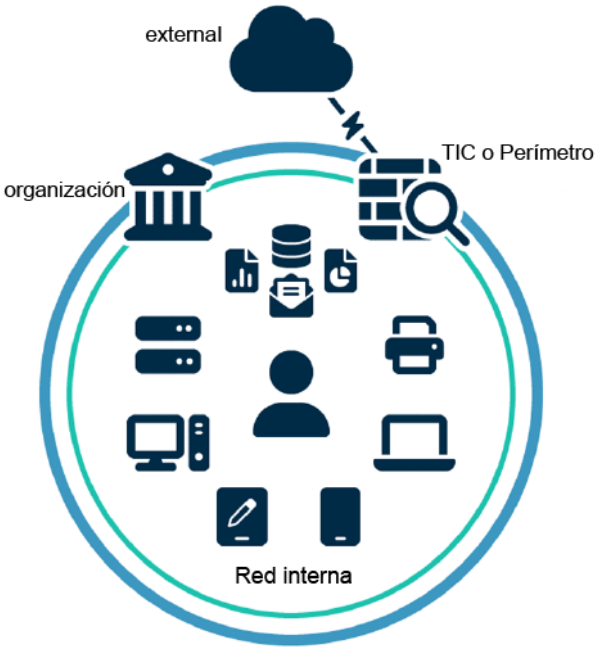

Figura 2: Red plana (no segmentada)

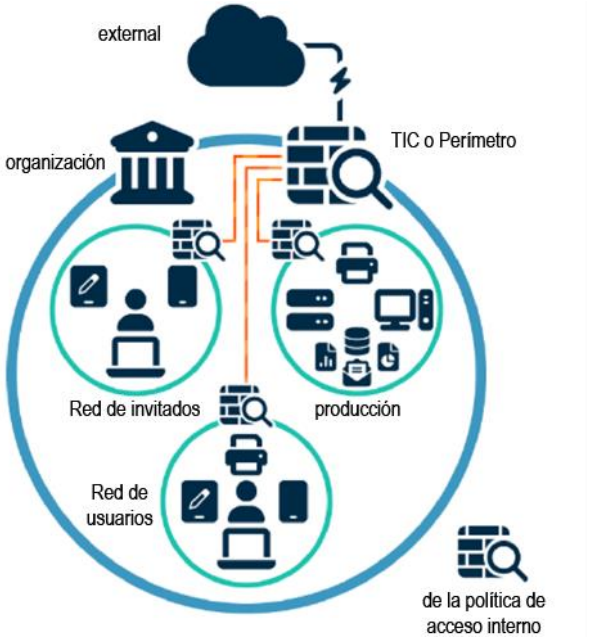

Figura 3: Red segmentada

- **Restrinja el uso de PowerShell a usuarios específicos caso por caso mediante el uso de la Política** de Grupo. Normalmente, sólo los usuarios o administradores que gestionan una red o un OS Windows pueden utilizar PowerShell. PowerShell es un lenguaje de script, un shell, de línea de comandos, multiplataforma que forma parte de Microsoft Windows. Los creadores de amenazas utilizan PowerShell para desplegar ransomware y ocultar sus actividades maliciosas. Para más información, consulte la Hoja informativa conjunta sobre Ciberseguridad Keeping PowerShell: Security Measure to Use and Embrace (Mantener PowerShell: Medida de seguridad para usar y adoptar).
    - Actualice Windows PowerShell o PowerShell Core a la última versión y desinstale todas las versiones anteriores de PowerShell.
    - Asegúrese de que las instancias de PowerShell, mediante el uso de la versión más reciente, tienen activados el registro de módulos, bloques de scripts y transcripciones (registro mejorado).
        - Los registros de Windows PowerShell anteriores a la versión 5.0 son inexistentes o no registran suficientes detalles para ayudar en las actividades empresariales de supervisión y respuesta a incidentes.
        - Los registros de PowerShell contienen datos valiosos, incluida la interacción histórica con el OS y el registro, así como posibles tácticas, técnicas y procedimientos del uso de PowerShell por parte de un creador de amenazas.
        - Dos registros que registran la actividad de PowerShell son el registro "PowerShell Windows Event" y el "PowerShell Operational". Las organizaciones autoras recomiendan activar estos dos registros de eventos de Windows con un período de retención de al menos 180 días.

        - Estos registros deben comprobarse periódicamente para confirmar si se han borrado los datos de registro o si se ha desactivado el registro. Ajuste el tamaño de almacenamiento permitido para ambos registros lo más grande posible.

- **Proteja los controladores de dominio (DC)**. Los delincuentes a menudo utilizan los DC como punto de partida para propagar el ransomware por toda la red. Para proteger los DC:
    - Utilice la última versión de Windows Server soportada por su organización en los DC. Las versiones más recientes del OS Windows Server tienen integradas más funciones de seguridad, incluido para Active Directory. Para obtener orientación sobre la configuración de las funciones de seguridad disponibles, consulte Best Practices for Securing Active Directory en Microsoft.
        - Las organizaciones autoras recomiendan utilizar Windows Server 2019 o superior y Windows 10 o superior, ya que cuentan con funciones de seguridad, como las protecciones LSASS con Windows Credential Guard, Windows Defender y Antimalware Scan Interface (AMSI), no incluidas en el sistema operativo anterior.
    - Asegúrese de aplica parches con regularidad a los DC. Aplique parches para vulnerabilidades críticas lo antes posible.
    - Utilice herramientas de pruebas de penetración de código abierto, como BloodHound, para verificar la seguridad del controlador de dominio.
    - Asegúrese de que se instala el mínimo software o agentes en los DC, ya que pueden aprovecharse para ejecutar códigos arbitrarios en el sistema.
    - Restrinja el acceso a los DC al grupo de Administradores. Los usuarios dentro de este grupo deben ser limitados y tener cuentas separadas utilizadas para operaciones diarias con permisos no administrativos. Para obtener más información, consulte Securing Active Directory Administrative Groups and Account en Microsoft.
        - Las cuentas de administrador designadas sólo deben utilizarse con fines administrativos. Asegúrese de que en los DC no se revisen correos electrónicos, se navegue por Internet ni se realicen otras actividades de alto riesgo.
    - Configure los cortafuegos del host del DC para impedir el acceso a Internet. Normalmente, los DC no necesitan acceso directo a Internet. Los servidores con conectividad a Internet pueden utilizarse para extraer las actualizaciones necesarias en lugar de permitir el acceso a Internet a los DC.
    - Implemente una solución de gestión de acceso privilegiado (PAM) en los DC para ayudar a gestionar y supervisar el acceso privilegiado. Las soluciones de PAM también pueden registrar y alertar del uso para detectar actividades inusuales.
    - Considere desactivar o limitar la Autenticación NTLM y WDigest, si es posible. Incluya su uso como criterio para dar prioridar a la actualización de sistemas heredados o para segmentar la red. En su lugar, utilice protocolos de federación modernos (por ejemplo, SAML, OIDC o Kerberos) para la autenticación con cifrado AES-256 bits https://cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf. Si NTLM debe estar habilitado:

        - Active la Protección ampliada para autenticación (EPA) a fin de evitar algunos ataques de retransmisión NTLM. Para obtener más información, consulte Mitigating NTLM Relay Attacks on Active Directory Certificate Services (AD CS) en Microsoft.
        - Active la auditoría NTLM para garantizar que sólo se envían respuestas NTLMv2 a través de la red. Deben adoptarse medidas para garantizar que se rechazan las respuestas LM y NTLM, si es posible.
    - Habilite protecciones adicionales para la Autenticación LSA a fin de evitar la inyección de código capaz de adquirir credenciales del sistema. Antes de habilitar estas protecciones, ejecute auditorías contra `lsass.exe` para asegurarse de conocer los programas que se verán afectados por la habilitación de esta protección.

- **Conserve y proteja adecuadamente los registros de dispositivos de red, hosts locales y servicios** en la nube Esto apoya la clasificación y la solución de eventos de ciberseguridad. Los registros pueden ser analizados para determinar el impacto de los eventos y determinar si se ha producido un incidente [CPG 2.T].
    - Establezca una gestión centralizada de registros mediante el uso de una herramienta de gestión de eventos e información de seguridad [CPG 2.U]. Esto permitirá a una organización correlacionar los registros de los dispositivos de seguridad de la red y del host. Al revisar los registros de múltiples fuentes, una organización puede clasificar un evento individual y determinar su impacto en la organización.
    - Mantenga y realice copias de seguridad de los registros de los sistemas críticos durante un mínimo de un año, si es posible.

- **Establezca una línea de base de seguridad del tráfico de red normal y ajuste los dispositivos de red para detectar comportamientos anormales**. Ajuste los productos basados en host a fin de detectar binarios anormales, movimientos laterales y técnicas de persistencia.
    - Considere la posibilidad de utilizar el registro de transacciones empresariales, como el registro de la actividad relacionada con aplicaciones específicas o críticas, para el análisis del comportamiento.

- **Realizar evaluaciones periódicas para** garantizar que los procesos y procedimientos están actualizados y pueden ser seguidos por el personal de seguridad y los usuarios finales.

Parte 2: Lista de comprobación de la respuesta al ransomware y la extorsión de datos

Si su organización es víctima de ransomware, siga su IRP aprobado. Las organizaciones autoras recomiendan encarecidamente responder utilizando la siguiente lista de comprobación. Asegúrese de seguir los **tres primeros pasos en secuencia.**

Las organizaciones autoras no recomiendan paga rescates. Pagar el rescate no garantizará que sus datos se descifren, que sus sistemas o datos dejen de estar en peligro o que sus datos no se filtren.

Además, el pago de rescates puede plantear riesgos de sanciones. Para obtener información sobre los posibles riesgos de sanciones, véase el memorando de la Foreign Assets Control (Oficina de Control de Activos Extranjeros) (OFAC) del Department of the Treasury (Departamento del Tesoro) de Estados Unidos de septiembre de 2021, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments El aviso actualizado establece que la OFAC del Department of the Treasury consideraría "factores atenuantes" en las acciones de aplicación relacionadas. Póngase en contacto con su oficina local del FBI, en consulta con la OFAC, para obtener orientación sobre los factores atenuantes de la sanción después de un ataque.

Detección y análisis

Consulte las mejores prácticas y referencias que figuran a continuación para ayudar a manejar el riesgo que plantea el ransomware y apoyar la respuesta coordinada y eficaz de su organización ante un incidente de ransomware. Aplique estas prácticas en la mayor medida posible en función de la disponibilidad de recursos de la organización.

- ☐ **1. Determine qué sistemas se han visto afectados y aíslelos inmediatamente.**
  - ☐ Si varios sistemas o subredes parecen afectados, desconecte la red a nivel de conmutador. Puede que no sea factible desconectar sistemas individuales durante un incidente.
  - ☐ Dé prioridad al aislamiento de los sistemas críticos que son esenciales para las operaciones diarias.
  - ☐ Si no es posible desconectar la red temporalmente de forma inmediata, localice el cable de red (por ejemplo, ethernet) y desconecte los dispositivos afectados de la red o retírelos de la Wi-Fi para contener la infección.
  - ☐ En el caso de los recursos en la nube, realice una imagen de los volúmenes para obtener una copia en un momento dado que pueda revisarse posteriormente para una investigación forense.
  - ☐ Después de un ataque inicial, los delincuentes pueden monitorear la actividad o las comunicaciones de su organización para entender si sus acciones han sido detectadas. Aísle los sistemas de forma coordinada y utilice métodos de comunicación fuera de banda, como llamadas telefónicas, para evitar que los delincuentes sepan que han sido descubiertos y que se están tomando medidas de mitigación. No hacerlo podría provocar que los delincuentes se muevan lateralmente para preservar su acceso o desplieguen ransomware ampliamente antes de que las redes queden sin conexión.

☐ **2. Apague los dispositivos si no puede desconectarlos de la red a fin de evitar una mayor propagación de la infección del ransomware.**

Nota: Este paso evitará que su organización mantenga artefactos de infección de ransomware y posibles pruebas almacenadas en la memoria volátil.**Solo debe llevarse a cabo si no es posible apagar temporalmente la red o desconectar los hosts afectados de la red por** otros medios.

☐ **3. Clasifique los sistemas afectados para su restauración y recuperación.**

- □ Identifique y dé prioridad a los sistemas críticos para su restauración en una red limpia y confirme la naturaleza de los datos alojados en los sistemas afectados.
    - Dé prioridad a la restauración y recuperación con base en una lista predefinida de activos críticos que incluya los sistemas de información fundamentales para la salud y la seguridad, la generación de ingresos u otros servicios críticos, así como los sistemas de los que dependen.
- □ Lleve un registro de los sistemas y dispositivos que no se perciben como afectados, de modo que puedan ser despriorizados para su restauración y recuperación. De este modo, su organización podrá retomar su actividad de forma más eficiente.

☐ **4. Revise los sistemas de detección o prevención existentes en la organización (por ejemplo, antivirus, EDR, IDS, sistema de prevención de intrusiones) así como los registros.** Esto puede poner de manifiesto la existencia de otros sistemas o malware implicados en las primeras fases del ataque.

- □ Busque pruebas de malware "dropper" precursor, como Bumblebee, Dridex, Emotet, QakBot o Anchor Un evento de ransomware puede ser la prueba de un ataque de red anterior no resuelto.
    - Los operadores de estas variantes avanzadas de malware suelen vender el acceso a una red. En ocasiones, los delincuentes utilizan este acceso para exfiltrar datos y amenazan con hacerlos públicos antes de pedir un rescate por la red para extorsionar a la víctima y presionarla para que pague.
    - Los delincuentes suelen soltar variantes de ransomware para ocultar la actividad posterior al ataque. Hay que tener cuidado de identificar este tipo de malware "dropper" antes de reconstruir las copias de seguridad para evitar que continúen las amenazas.

☐ **5. Reúnase con su equipo para desarrollar y documentar una comprensión inicial de lo ocurrido con base en el análisis inicial.**

☐ **6. Iniciar actividades de caza de amenazas.**

- □ En el caso de entornos empresariales, verifique:
    - Cuentas AD recién creadas o cuentas con privilegios escalados y actividad reciente relacionada con cuentas privilegiadas como Administradores de Dominio.

- Inicios de sesión anómalos en dispositivos VPN u otros inicios de sesión sospechosos.
- Modificaciones en los puntos finales que puedan afectar a las copias de seguridad, las instantáneas, el registro en diario de los discos o las configuraciones de arranque. Busque el uso anómalo de herramientas integradas de Windows como `bcdedit.exe`, `fsutil.exe` (deletejournal), `vssadmin.exe, wbadmin.exe y wmic.exe` (shadowcopy o shadowstorage). El uso indebido de estas herramientas es una técnica habitual del ransomware para impedir la recuperación del sistema.
- Indicios de la presencia de Cobalt Strike Beacon/Client. Cobalt Strike es un paquete de software comercial de pruebas de penetración Los delincuentes suelen nombrar los procesos de Windows de Cobalt Strike con los mismos nombres que los procesos legítimos de Windows para ofuscar su presencia y complicar las investigaciones.
- Señales de cualquier uso inesperado de software de supervisión y gestión remotas (RMM) (incluidos los ejecutables portátiles que no están instalados). Los delincuentes suelen utilizar el software de RMM para mantener la persistencia.
- Cualquier ejecución inesperada de PowerShell o uso del paquete PsTools.
- Signos de enumeración de credenciales AD y/o LSASS que se transfieren (por ejemplo, Mimikatz o `NTDSutil.exe`).
- Señales de comunicaciones inesperadas de punto final a punto final (incluidos los servidores).
- Posibles indicios de exfiltración de datos de la red. Entre las herramientas comunes para la exfiltración de datos se incluyen Rclone, Rsync, varios servicios de almacenamiento de archivos basados en web (también utilizados por los creadores de amenazas para implantar malware/herramientas en la red afectada) y FTP/SFTP.
- Servicios recién creados, tareas programadas inesperadas, software instalado inesperado, etc.

☐ En el caso de los entornos de nube:

- Habilite herramientas para detectar y evitar modificaciones en los recursos de IAM, seguridad de red y protección de datos.
- Utilice la automatización para detectar problemas comunes (por ejemplo, desactivación de funciones, introducción de nuevas normas de cortafuegos) y tome medidas automatizadas en cuanto se produzcan. Por ejemplo, si se crea una nueva norma de cortafuegos que permite el tráfico abierto (`0.0.0.0/0`), se puede emprender una acción automatizada para desactivar o eliminar esta norma y enviar notificaciones al usuario que la creó, así como al equipo de seguridad para su conocimiento. Esto ayudará a evitar la fatiga por alertas y permitirá al personal de seguridad centrarse en los problemas críticos.

Informes y notificaciones

Nota: Consulte la sección Información de contacto al final de esta guía para obtener información detallada sobre cómo reportar y notificar incidentes de ransomware.

- ☐ **7.** Siga los requisitos de notificación descritos en su plan de comunicación y respuesta a incidentes cibernéticos **para involucrar a los equipos internos y externos y a las partes interesadas** con un entendimiento de lo que pueden proporcionar para ayudarle a mitigar, responder y recuperarse del incidente.
  - ☐ Comparta la información de que disponga para recibir asistencia oportuna y pertinente. Mantenga informados a la dirección y a los líderes principales mediante actualizaciones periódicas a medida que evolucione la situación. Las partes interesadas relevantes pueden incluir su departamento de TI, proveedores de servicios de seguridad gestionados, compañía de seguros cibernéticos y líderes departamentales o electos [CPG 4.A].
  - ☐ Reporte el incidente y considere la posibilidad de solicitar ayuda a la CISA, a la oficina local del FBI, al Centro de Denuncias de Delitos en Internet (IC3) del FBI o a la oficina local del Servicio Secreto de EE. UU.
  - ☐ Según proceda, coordínese con el personal de comunicación e información

Si se necesita una identificación o análisis ampliados, CISA, MS-ISAC y las fuerzas de seguridad locales, estatales o federales pueden estar interesadas en cualquiera de los siguientes datos que su organización determine que puede compartir legalmente:

- Archivo ejecutable recuperado.
- Copias del archivo readme - NO ELIMINE el archivo o puede que no sea posible el descifrado.
- Captura de memoria viva (RAM) de sistemas con signos adicionales de ataque (uso de kits de exploits, actividad RDP, archivos adicionales encontrados localmente).
- Imágenes de sistemas infectados con signos adicionales de ataque (uso de kits de exploits, actividad RDP, archivos adicionales encontrados localmente).
- Muestras de malware.
- Nombres de malware identificados en su red.
- Muestras de archivos cifrados.
- Archivos de registro (por ejemplo, registros de eventos de Windows de sistemas en riesgo, registros de cortafuegos).
- Scripts de PowerShell encontrados que se han ejecutado en la red.
- Cuentas de usuario creadas en AD o máquinas añadidas a la red durante la explotación.
- Direcciones de correo electrónico utilizadas por los atacantes y cualquier correo electrónico de phishing asociado.
- Otras cuentas de comunicación utilizadas por los atacantes.
- Una copia de la nota de rescate.
- Monto del rescate y si se pagó.
- Monederos Bitcoin utilizados por los atacantes.
- Monederos Bitcoin utilizados para pagar el rescate, si procede.
- Copias de cualquier comunicación con los atacantes.

pública para garantizar que se comparte información precisa internamente con su organización y de forma externa con el público.

- ☐ **8.** Si el incidente ha dado lugar a una violación de datos, **siga los requisitos de notificación establecidos en sus planes de comunicación y respuesta a incidentes cibernéticos.**

Contención y erradicación

Si no parece posible adoptar medidas iniciales de mitigación:

- ☐ **9. Tome una imagen del sistema y una captura de memoria de una muestra de los dispositivos afectados (por ejemplo, estaciones de trabajo, servidores, servidores virtuales y servidores en la nube).** Recopile todos los registros pertinentes, así como muestras de cualquier binario de malware "precursor" y observables asociados o indicadores de ataque (por ejemplo, direcciones IP sospechosas de comando y control, entradas de registro sospechosas u otros archivos relevantes detectados). Los contactos que se indican a continuación pueden ayudarle a realizar estas tareas.
  - ☐ Conserve las pruebas de naturaleza muy volátil o de conservación limitada, para evitar su pérdida o manipulación (por ejemplo, la memoria del sistema, los registros de seguridad de Windows, los datos del buffer de registro de los cortafuegos).

Previa solicitud voluntaria, la CISA y MS-ISAC (para organizaciones SLTT) pueden ayudar con el análisis de correos electrónicos de phishing, medios de almacenamiento, registros y/o malware de forma gratuita para ayudar a las organizaciones a comprender la causa root de un incidente.

- CISA - Centro de Análisis Avanzado de Malware: malware.us-cert.gov/
- MS-ISAC - Plataforma de análisis de código malicioso (sólo organizaciones SLTT): cisecurity.org/spotlight/cybersecurity-spotlight-malware-analysis/

- ☐ **10. Consulte a las fuerzas de seguridad federales, incluso si es posible adoptar medidas de mitigación, sobre los posibles descifradores** disponibles, ya que los investigadores de seguridad pueden haber descubierto fallas de cifrado para algunas variantes de ransomware y haber publicado herramientas de descifrado o de otro tipo.

A fin de seguir tomando medidas para contener y mitigar el incidente:

- ☐ **11. Busque orientación fiable** (por ejemplo, publicada por fuentes como el Gobierno de EE. UU., MS-ISAC o un proveedor de seguridad de confianza) para la variante de ransomware concreta y siga cualquier paso adicional recomendado a fin de identificar y contener los sistemas o redes que se haya confirmado que están afectados.
  - ☐ Elimine o desactive la ejecución de los binarios conocidos del ransomware; esto minimizará el daño y el impacto en sus sistemas. Elimine otros valores de registro y archivos asociados conocidos.

- ☐ **12. Identifique los sistemas y cuentas implicados en la violación inicial.** Esto puede incluir cuentas de correo electrónico.

- ☐ **13.** Con base en los detalles de la violación o ataque determinados anteriormente, **contenga los sistemas asociados que puedan utilizarse para un acceso no autorizado posterior o continuado.** Las violaciones a menudo implican la exfiltración masiva de credenciales. La protección de las redes y otras fuentes de información del acceso no autorizado continuado basado en credenciales puede incluir:
    - ☐ La desactivación de las redes privadas virtuales, los servidores de acceso remoto, los recursos de inicio de sesión único y los activos basados en la nube u otros activos disponibles al público.

- ☐ **14.** Si una estación de trabajo infectada está cifrando datos del lado del servidor, **siga los pasos de identificación rápida del cifrado de datos del lado del servidor.**
    - ☐ Revise Administración de equipos > Sesiones y las listas de Archivos abiertos en los servidores asociados para determinar el usuario o sistema que accede a esos archivos.
    - ☐ Revise las propiedades de los archivos cifrados o las notas de rescate para identificar usuarios específicos que puedan estar asociados a la propiedad de los archivos.
    - ☐ Revise el registro de eventos de `TerminalServices-RemoteConnectionManager` para comprobar si hay conexiones de red RDP satisfactorias.
    - ☐ Revise el registro de seguridad de Windows, los registros de eventos de SMB y los registros relacionados que puedan identificar eventos significativos de autenticación o acceso.
    - ☐ Ejecute un software de captura de paquetes, como Wireshark, en el servidor afectado con un filtro para identificar las direcciones IP implicadas en la escritura activa o el cambio de nombre de archivos (por ejemplo, `smb2.filename contains cryptxxx`).

- ☐ **15. Realice un análisis ampliado para identificar los mecanismos de persistencia "outside-in" e "inside-out".**
    - ☐ La persistencia "outside-in" puede incluir el acceso autenticado a sistemas externos a través de cuentas fraudulentas, puertas traseras en sistemas perimetrales, explotación de vulnerabilidades externas, etc.
    - ☐ La persistencia "inside-out" puede incluir implantes de malware en la red interna o una variedad de modificaciones al estilo "living-off-the-land" (por ejemplo, el uso de herramientas comerciales de pruebas de penetración como Cobalt Strike; el uso del paquete PsTools, incluido PsExec, para instalar y controlar malware de forma remota y recopilar información relativa a los sistemas Windows o realizar su gestión remota; el uso de scripts de PowerShell).
    - ☐ La identificación puede implicar el despliegue de soluciones EDR, auditorías de cuentas locales y de dominio, revisión de los datos encontrados en los sistemas de registro centralizados o un análisis forense más profundo de sistemas específicos una vez que se ha trazado el movimiento dentro del entorno.

- ☐ **16. Reconstruya los sistemas con base en la priorización de los servicios** críticos (por ejemplo, salud y seguridad o servicios generadores de ingresos), utilizando imágenes estándar preconfiguradas, si es posible. Utilice la infraestructura como plantillas de código para reconstruir los recursos en la nube.

- ☐ **17. Solicite restablecimientos de contraseñas para todos los sistemas afectados y aborde cualquier vulnerabilidad asociada y brecha en la seguridad o visibilidad** una vez que el entorno haya sido completamente limpiado y reconstruido, incluyendo cualquier cuenta asociada afectada y la eliminación o corrección de mecanismos de persistencia maliciosos. Esto puede incluir la aplicación de parches, la actualización de software y la adopción de otras precauciones de seguridad no adoptadas anteriormente. Actualice las claves de cifrado gestionadas por el cliente según sea necesario.

- ☐ **18. La autoridad de TI o de seguridad de TI designada declara el incidente de ransomware finalizado** en función de los criterios establecidos, que pueden incluir la adopción de las medidas anteriores o la búsqueda de ayuda externa.

Recuperación y actividad posterior al incidente

- ☐ **19. Reconecte los sistemas y restaure los datos a partir de copias de seguridad cifradas sin conexión, con base en una priorización de los servicios críticos.**
  - □ Tenga cuidado de no reinfectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva Red de Área Local Virtual (VLAN) con fines de recuperación, asegúrese de que sólo se añaden sistemas limpios.

- ☐ **20. Documente las lecciones aprendidas del incidente y de las actividades de respuesta asociadas para** actualizar y perfeccionar las políticas, planes y procedimientos de la organización y orientar futuros ejercicios de los mismos.

- ☐ **21. Considere la posibilidad de compartir las lecciones aprendidas y los indicadores relevantes del ataque con la CISA o el ISAC de su sector para** beneficiar a otros dentro de la comunidad.

Información de contacto

En respuesta a cualquier incidente cibernético, las agencias federales llevarán a cabo la respuesta a las amenazas; la respuesta a los activos; y el apoyo de inteligencia y actividades relacionadas.

Qué puede esperar:

- Guía específica para ayudar a evaluar y corregir incidentes de ransomware.
- Asistencia remota para identificar el alcance del ataque y recomendaciones sobre estrategias de contención y mitigación adecuadas (en función de la variante de ransomware específica).
- Análisis de correos electrónicos de phishing, medios de almacenamiento, registros y malware basados en envíos voluntarios. Se pueden realizar análisis forenses de todo el disco en función de las necesidades.
- Asistencia en la realización de una investigación criminal, que puede implicar la recopilación de artefactos del incidente, incluidas imágenes del sistema y muestras de malware.

Contacto de respuesta federal de activos

A petición voluntaria, la respuesta de los activos federales incluye prestar asistencia técnica a las entidades afectadas para proteger sus activos, mitigar las vulnerabilidades y reducir los impactos de los incidentes cibernéticos; identificar otras entidades que puedan estar en riesgo y evaluar su riesgo a las mismas vulnerabilidades o similares; evaluar los riesgos potenciales para el sector o la región, incluidos los posibles efectos en cascada, y desarrollar cursos de acción para mitigar estos riesgos; facilitar el intercambio de información y la coordinación operativa con la respuesta a las amenazas; y proporcionar orientación sobre la mejor manera de utilizar los recursos y capacidades federales de manera oportuna y eficaz para acelerar la recuperación.

CISA:	cisa.gov/report Central@cisa.gov o llame al (888) 282-0870 Asesor de Ciberseguridad (cisa.gov/cisa-regions): [Introduzca el número de teléfono y la dirección de correo electrónico de su CSA local de CISA].
MS-ISAC:	Para SLTT, envíe un correo electrónico a soc@msisac.org o llame al (866) 787-4722

Contactos de respuesta federal a amenazas

A petición voluntaria, o previa notificación a los socios, la respuesta federal a la amenaza incluye realizar actividades de investigación policial y de seguridad nacional apropiadas en el lugar de la entidad afectada; recabar pruebas y recopilar información; proporcionar atribución; vincular incidentes relacionados; identificar otras entidades afectadas; identificar oportunidades de persecución de la amenaza y de interrupción; desarrollar y ejecutar cursos de acción para mitigar la amenaza inmediata; y facilitar el intercambio de información y la coordinación operativa con la respuesta de los activos.

FBI: fbi.gov/contact-us/field-offices [Introduzca el número de teléfono y la dirección de correo electrónico de su oficina local del FBI].

USSS: secretservice.gov/contact/field-offices/ [Introduzca el número de teléfono y la dirección de correo electrónico de su oficina local del USSS].

Otros contactos de respuesta federal

NSA: Cybersecurity Collaboration Center Services and Contact Information

Otros contactos de respuesta

Considere la posibilidad de completar la Tabla 1 para su uso en caso de que su organización se vea afectada por el ransomware. Considere la posibilidad de ponerse en contacto con estas organizaciones para obtener asistencia de mitigación y respuesta o para recibir una notificación.

Tabla 1: Información de los contactos de respuesta

Contactos de respuesta:		
Póngase en contacto con	**Información de contacto 24x7**	**Funciones y responsabilidades**
Equipo de seguridad informática/TI - Notificación centralizada de ciberincidentes		
Líderes departamentales o elegidos		
Fuerzas y cuerpos de seguridad estatales y locales		
Centro de Fusión		
Proveedores de servicios gestionados/de seguridad		
Ciberseguro		

RECURSOS

Recursos gratuitos de la CISA

- El intercambio de información con CISA y MS-ISAC (para organizaciones SLTT) es bidireccional. Esto incluye las mejores prácticas y la información de defensa de la red en relación con las tendencias y variantes del ransomware, así como el malware precursor del ransomware.
- Las evaluaciones técnicas u orientadas a las políticas ayudan a las organizaciones a comprender cómo pueden mejorar sus defensas para evitar la infección por ransomware: cisa.gov/cyber-resource-hub.
    - Las evaluaciones incluyen análisis de vulnerabilidades gratuito.
- Los ejercicios cibernéticos evalúan o ayudan a desarrollar un plan de respuesta a incidentes cibernéticos en el contexto de un escenario de incidente de ransomware: cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.
- Los asesores de ciberseguridad de CISA aconsejan sobre las mejores prácticas y lo conectan con los recursos de CISA para gestionar el ciberriesgo.
- Cyber Security Evaluation Tool (CSET) guía a los propietarios y operadores de activos a través de un proceso sistemático de evaluación de la tecnología operativa (OT) y de TI. CSET incluye la Ransomware Readiness Assessment (RRA), una autoevaluación basada en un conjunto escalonado de prácticas para ayudar a las organizaciones a evaluar en qué medida están equipadas para defenderse y recuperarse de un incidente de ransomware.

Contactos:

- SLTT y organizaciones del sector privado: CISA.JCDC@cisa.dhs.gov

Referencias rápidas sobre ransomware

- StopRansomware.gov: un sitio web gubernamental que ofrece recursos y alertas sobre ransomware.
- Security Primer - Ransomware (MS-ISAC): describe las campañas oportunistas y estratégicas de ransomware, los vectores de infección habituales y las recomendaciones de buenas prácticas.
- Institute for Security + Technology (IST) Blueprint for Ransomware Defense: un plan de acción para la mitigación, respuesta y recuperación del ransomware para pequeñas y medianas empresas.

Recursos adicionales

- NIST: Zero Trust Architecture
- CISA: Cloud Security Technical Reference Architecture
- CISA: Secure Cloud Business Applications (SCuBA) Project
- CISA: Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses
- CISA: Protecting Against Cyber Threats to Managed Service Providers and their Customers
- NSA: Mitigating Cloud Vulnerabilities (NSA)

DESCARGO DE RESPONSABILIDAD

La información y las opiniones contenidas en este documento se facilitan "tal cual" y sin garantías de ningún tipo. La referencia en este documento a cualquier producto, proceso o servicio comercial específico por su nombre comercial, marca registrada, fabricante u otro, no constituye ni implica su aprobación, recomendación o favorecimiento por parte del Gobierno de los Estados Unidos, y esta guía no se utilizará con fines publicitarios o de aprobación de productos.

OBJETIVO

Este documento se ha elaborado en cumplimiento de las misiones de ciberseguridad de los autores, incluidas sus responsabilidades de identificar y difundir amenazas, y de desarrollar y publicar especificaciones y mitigaciones de ciberseguridad. Esta información puede compartirse ampliamente para llegar a todas las partes interesadas apropiadas.